UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- - - - - - - - - - - - - - - - - -X

IN THE MATTER OF AN APPLICATION FOR A SEARCH WARRANT FOR:

THE PREMISES KNOWN AND DESCRIBED AS:
A. A VIVITAR DVR CAMCORDER WITH MICRO SD CARD
B. AN MLT DVR FOR SURVEILLANCE CAMERAS
C. AN ACER LAPTOP
D. A LACIE BRAND THUMB DRIVE
E. A SWANN BRAND SD CARD
F. MISCELLANEOUS CDS AND DVDS
G. A MOTOROLA BOOST CELL PHONE (BLUE) WITH MICRO SD CARD
H. A MICRO SD CARD READER WITH MICRO SD CARD
I. A GIGAWARE HARD DRIVE
J. A ZIP DRIVE, 100 USB EASY POWERED (BLUE)
K. A SANDISK FLASH DRIVE(4 GIGABYTES)
L. A METRO PCS CELL PHONE (BLACK) WITH MICRO SD CARD

12-712 M

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

- - - - - - - - - - - - - - - - - -X

EASTERN DISTRICT OF NEW YORK, SS:

ROBERT MANCENE, being duly sworn, deposes and states that he is a Special Agent with Department of Homeland Security, Homeland Security Investigations, duly appointed according to law and acting as such.

Upon information and belief, there is probable cause to believe that there is located in THE PREMISES KNOWN AND DESCRIBED AS A VIVITAR DVR CAMCORDER WITH MICRO SD CARD(“PREMISES A”); AN MLT DVR FOR SURVEILLANCE CAMERAS (“PREMISES B”); AN ACER LAPTOP

("PREMISES C"); A LACIE BRAND THUMB DRIVE ("PREMISES D"); A SWANN BRAND SD CARD ("PREMISES E"); MISCELLANEOUS CDS AND DVDS ("PREMISES F"); A MOTOROLA BOOST CELL PHONE (BLUE) WITH MICRO SD CARD ("PREMISES G"); A MICRO SD CARD READER WITH MICRO SD CARD ("PREMISES H"); A GIGAWARE HARD DRIVE ("PREMISES I"); A ZIP DRIVE, 100 USB EASY POWERED (BLUE) ("PREMISES J"); A SANDISK FLASH DRIVE (4 GIGABYTES) ("PREMISES K"); A METRO PCS CELL PHONE (BLACK) WITH MICRO SD CARD ("PREMISES L"), all seized from 559 Newark Avenue, Jersey City, New Jersey on June 3, 2012 (collectively, the "PREMISES"), which are currently located within the Eastern District of New York, things described in the Attachment, which constitute evidence, fruits and instrumentalities of the crimes of extortion, coercion and enticement to travel for the purpose of engaging in illegal sexual activity, coercion and enticement of a minor for the purpose of engaging in illegal sexual activity, production of child pornography and possession of child pornography, in violation of 18 U.S.C. §§ 875, 2422(a), 2422(b), 2251(a) and 2252(a)(4)(B), respectively.

The source of your deponent's information and the grounds for his belief are as follows:

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"). I have been an HSI Special Agent or its predecessor agencies since

1996. For approximately the past three years, I have been assigned to an HSI Child Exploitation Group in New York City. In that capacity, I have conducted investigations into federal crimes relating to the sex trafficking of minors, Mann Act violations and child pornography. As an HSI Special Agent, I have conducted or participated in surveillance, the execution of search warrants, debriefings of informants, victims and witnesses, and have participated in investigations that included the interception of wire communications. Through my training, education and experience, I have become familiar with the manner in which individuals conduct and conceal activity involving the sexual exploitation of children. I am familiar with the facts and circumstances of this investigation from: (a) my personal participation in the investigation; (b) reports made to me by other law enforcement authorities and forensic professionals; and (c) review of records and reports.

2. Unless otherwise noted, wherever in this affidavit I assert that a statement was made, the information was provided by another law enforcement officer or witness who may have had either direct or hearsay knowledge of that statement and to whom I or others have spoken or whose reports I have read and reviewed. Such statements are among many statements made by others and are stated in substance and in part unless otherwise indicated. Since this affidavit is being submitted for the

limited purpose of securing a search warrant, I have not included details of every aspect of the investigation. Facts not set forth herein are not being relied on in reaching my conclusion that the requested warrant should be issued. Nor do I request that this Court rely on any facts not set forth herein in reviewing this application.

I. PROBABLE CAUSE

3. In or about March 2012, I was notified by New York City Police Department ("NYPD") detectives that a 15-year-old girl ("Jane Doe") from Brooklyn, New York had reported that she was sexually assaulted several days earlier at 559 Newark Avenue, Jersey City, New Jersey by a man named "John."

Interview of Jane Doe

4. On or about April 5, 2012, at my request, Jane Doe was interviewed by a clinical forensic specialist. During the interview, Jane Doe stated, in substance and in part:

a. Prior to March 17, 2012, she had posted an ad on Craigslist indicating that she was a "Teen in need of a afterschool & weekend job (NYC)."

b. In early March, someone named "John Archambeault" (who was subsequently identified as GREGORY SCHAFFER) responded to her ad by email, stating that he was "looking for part time help in my store in Newport mall in Jersey

city" [sic].[1]

c. In subsequent email communication, SCHAFFER and Jane Doe arranged to meet to further discuss a purported employment opportunity for Jane Doe in one of SCHAFFER's "stores." SCHAFFER told Jane Doe that he owned retail stores in the Newport Mall, including American Eagle Outfitters, Victoria's Secret, Champs Sports and Spencer Gifts. Schaffer asked for Jane Doe's age, and she told him that she was 15 years old. He also asked whether she would be coming to New Jersey with her parents or alone, and asked her to send a photograph for "security."

d. On or about March 17, 2012, Jane Doe traveled from her home in Brooklyn to SCHAFFER's office in Jersey City, New Jersey, accompanied by a male friend, who was also a minor ("Friend"). Once inside the office suite area, SCHAFFER took Jane Doe into a private office area and closed the door, leaving the Friend in the waiting area.

e. During the March 17th meeting, SCHAFFER told Jane Doe that he was probably going to have her work in his Victoria's Secret store. SCHAFFER also asked Jane Doe whether she was sexually active, which she stated she was, and whether she used drugs. SCHAFFER gave Jane Doe paperwork for her great-grandmother, who is Jane Doe's guardian, to sign.

f. That night, Jane Doe's great-grandmother

[1] The quoted excerpts from the emails are taken from the actual

signed the paperwork and Jane Doe emailed SCHAFFER to advise him that the paperwork was signed. SCHAFFER responded by email, asking her if she could return the next day with the paperwork. He added that she should come alone because it might be her first day of work.

g. On or about March 18, 2012, Jane Doe again traveled from her home in Brooklyn to SCHAFFER's office, this time alone. During the March 18th meeting, SCHAFFER gave Jane Doe a "confidentiality agreement," which he asked her to sign. SCHAFFER also gave Jane Doe an employment contract to sign. Jane Doe signed both agreements without reading them carefully.

h. After she had signed them, SCHAFFER informed Jane Doe that by signing them, she had agreed to have sex with him. SCHAFFER had Jane Doe try on "outfits" for him, which included a bathing suit, and took pictures of Jane Doe in the bathing suit. Some time later, SCHAFFER removed his pants, revealing that he was wearing a Speedo bathing suit, and told Jane Doe that he wanted to photograph them together. At this point, Jane Doe told SCHAFFER that she did not feel comfortable.

i. SCHAFFER asked Jane Doe if she had a boyfriend, to which she responded that she did and that he was 17 years old. SCHAFFER threatened to "report" the boyfriend -- impliedly because Jane Doe and the boyfriend were having sex --

---

email messages between Schaffer and Jane Doe.

if she broke the contract. SCHAFFER also threatened to sue Jane Doe's great-grandmother for breach of contract.

j. After having Jane Doe lie on his desk, SCHAFFER took a white pill and inserted it into her vagina, telling her it was "birth control."[1] Jane Doe asked SCHAFFER to use a condom, which he took from the drawer in his desk and put on. SCHAFFER then had sexual intercourse with Jane Doe. During the sexual intercourse, Jane Doe attempted to reach for her cell phone several times, but SCHAFFER blocked her hand.

k. Afterward, SCHAFFER told Jane Doe that he would remove the sex part of the contract and gave her a new contract. SCHAFFER shredded the contract that Jane Doe had signed. SCHAFFER told Jane Doe not to speak to anyone about their sexual encounter because that would be a breach of their confidentiality agreement.

l. Jane Doe did not want to have sexual intercourse with SCHAFFER, but was afraid of being sued.

m. When Jane Doe returned home, she told her boyfriend ("Boyfriend") what had happened. The Boyfriend became upset and tore up and disposed of the new contract that SCHAFFER had given to Jane Doe.

n. During the time that Jane Doe was at 559

[1] White pills were seized on June 3, 2010 pursuant to a search warrant and further research indicates that they are most likely spermicide.

Newark Avenue, Jersey City, New Jersey with SCHAFFER, there was a black camera or video camera on a tripod in SCHAFFER's office. The black camera was in the room when Jane Doe was changing into the bathing suit, and then SCHAFFER replaced it with a red camera after she had changed into the bathing suit. SCHAFFER removed a memory card from the black camera and inserted it into the laptop on SCHAFFER's desk. Jane Doe stated that SCHAFFER put the red camera away during the sexual intercourse.

Interview with the Friend

5. On May 29 and 30, 2012, I interviewed the Friend, who reported, in part and substance, that he had accompanied Jane Doe to an office in Jersey City for a job interview. The Friend stated that the building in which the office was located bore a sign for a bail bonds business. The Friend stated that Jane Doe and he were met by a man when they entered the office area in the building and that the man took Jane Doe into an interior office through the first door on the left. The Friend remained in the waiting area. Jane Doe was in the interior office with the man for about 45 minutes. After Jane Doe and the Friend had left the building, Jane Doe told the Friend that she had gotten the job and that the man had asked her to return later. When the Friend called Jane Doe the next day, she told the Friend that she was approaching the same Jersey City office building. A couple days later, Jane Doe told the Friend that the man in the Jersey City

office had raped her.

Interview of the Boyfriend

6. On May 29 and 30, 2012, I interviewed the Boyfriend, who reported, in part and substance, that after Jane Doe had returned from her second trip to Jersey City, she called him. She was crying and asked him if he loved her, to which the Boyfriend responded affirmatively and asked her what had happened. Jane Doe told the Boyfriend that the job offer had turned into something that she did not want. She explained that the man had taken pictures of her in lingerie and that the man had a photographer friend to whom he could send the photos. But, the man later said that he would post the photos on the Internet if Jane Doe did not have sex with him. Jane Doe also said that she had signed a contract that she thought was for a retail job, but that the man later told her that under the contract she was legally bound to have sex with him, or else he could sue her. Jane Doe further stated that she had sex with the man because she feared that her great-grandmother could get in trouble for letting Jane Doe travel by herself to Jersey City. When the Boyfriend later saw Jane Doe, she showed him the contract. Out of anger, the Boyfriend ripped it up and disposed of it. Jane

Doe also showed the Boyfriend a business pen from Schaffer that indicated that SCHAFFER's last name is "Archambeault."

Photo Identification of SCHAFFER

7. Jane Doe and the Friend both identified a photograph of SCHAFFER from a photo array.

Records Checks

8. Publicly available corporate records indicate that there are, in fact, Victoria's Secret, American Eagle, Champs Sports and Spencer Gifts stores at the Newport Center Mall in Jersey City. However, each of these stores is corporately, and not individually, owned and operated. These records further indicate that none of the managers at these stores is "John Archambeault" or Greg Schaffer.

Search of Defendant's Office

9. On June 3rd, 2012, HSI agents executed a search warrant, issued by a federal judge in the District of New Jersey, for SCHAFFER's office. During the search, agents recovered, among other things, PREMISES A-L, a folder containing a letter from Jane Doe, computer-printed photographs of teenage-appearing girls wearing bathing suits or naked, condoms (both used and unused), sexual paraphernalia, including lubricants, white pills, handcuffs and sex toys, employment applications, some of which include questions about the applicant's sexual activity and dating status, and a document entitled "Sex Contract."

a. In addition, agents also recovered a document that appeared to be a letter bearing a female name ("JANE DOE 2") at the top. The document reads, in substance and in part:

> JANE DOE 2
>
> HERE IS THE DEAL, I HAVE ALL THE STUFF YOU POSTED ONLINE AND EVEN PHOTOS OF YOU NUDE. I KNOW YOU HAVE BEEN GIVING YOUR PHONE NUMBER OUT AND I KNOW A LOT MORE(LIKE HOW YOU KEEP SAYING YOU WANT TO GET PREGNANT BY ANYONE). NOW HERE IS THE DAL I HAVE ENOUGH TO HAVE YOU PUT IN A PSYCO WARD, YOUR BROTHER AND SISTER REMOVED AND YOUR MOM LOCKED UP FOR 5 YEARS. YOU WILL BE NEVER ALLOWED TO SEE ANY OF YOUR FRIENDS AGAIN ([female name] OR ANYONE ELSE) BECAUSE YOU WILL BE ADOPTED HERE TO DO, I ALSO HAVE SOME CASHIERS CHECKS IN YOUR NAME (THER ARE THE SAME AS CASH). YOU ARE GOING TO LOOK AT THE AMOUNT IT IS MADE OUT FOR AND PICK 1 OR 2 THINGS FROM THE LIST YOU WILL DO OR LET BE DONE FOR THAT PRICE. IF I AGREE TO IT YOU KEEP IT THE CHECK AND WHAT YOU PICK GETS DONE. WE WILL KEEP GOING UNTILL YOU HAVE ALL THE CHECKS AND ALL OR MOST ITEMS ARE DONE. IF YOU CAN GUESS WHAT AMOUNTS LISTED ARE REAL YOU GET IT WITH OUT DOING ANYTHING. IF YOU GET IT WRONG YOU MUST DO SOMETHING FROM THE LIST (MY CHOICE).

Following that is a list of amounts of United States Currency from $1000 to $10 million. Following that there is list of 16 sexual acts, the last item on the list is "RAPE FOR REAL *****". A post-script reads "*** this is what will happen if you do not pick from the list and we do not agree. It will also happen if you refuse to do any of the above." Based on this note, the photographs of teenagers other than JANE DOE, the fraudulent employment applications, and the "Sex Contract", I believe the defendant was victimizing individuals prior

to JANE DOE.

10. Based upon the above facts, I have probable cause to believe that PREMISES A-L contain information and evidence relating to extortion, coercion and enticement to travel for the purpose of engaging in illegal sexual activity, coercion and enticement of a minor for the purpose of engaging in illegal sexual activity, production of child pornography and possession of child pornography, in violation of 18 U.S.C. §§ 875, 2422(a), 2422(b), 2251(a) and 2252(a)(4)(B), respectively.

11. The premises are currently located at offices of the United States Secret Service in Melville, New York.

II. TECHNICAL BACKGROUND

12. Based on the foregoing and below information, I submit that there is probable cause to believe those records will be stored on the PREMISES, including the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear;

rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the storage medium that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media - in particular, computers' internal hard drives - contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

13. As further described in Attachment B, this application seeks permission to locate not only computer files

that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be stored on the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to

the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

14. I know that when an individual uses a computer to extort, to facilitate the coercion and enticement to travel for the purpose of engaging in illegal sexual activity, to facilitate the coercion and enticement of interstate travel of a minor for the purpose of engaging in illegal sexual activity and to produce child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

III. CONCLUSION

15. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the PREMISES there exists fruits, instrumentalities and evidence crimes of extortion, coercion and enticement to travel for the purpose of engaging in illegal sexual activity, coercion and enticement of a minor for the purpose of engaging in illegal sexual activity, production of child pornography and possession of child pornography, in violation of 18 U.S.C. §§ 875, 2422(a), 2422(b), 2251(a) and 2252(a)(4)(B), respectively. Accordingly, a search warrant is requested.

WHEREFORE, your deponent respectfully requests that the requested search warrant be issued for THE PREMISES.

S/ Robert Mancene

_____
Robert Mancene
Special Agent
Homeland Security
Investigations

Sworn to and subscribed before me
this 31st day of July, 2012

S/ Joan Azrack

_____
THE HONORABLE JOAN M. AZRACK
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

As described above, this application seeks permission to search:

A. A Vivitar DVR Camcorder with Micro SD card
B. A MLT DVR for surveillance cameras
C. An Acer laptop
D. A LaCie brand thumb drive
E. A Swann brand SD card
F. Miscellaneous CDs and DVDs
G. A Motorola Boost Cell Phone with Micro SD card (blue)
H. A Micro SD Card Reader with Micro SD card
I. A Gigaware hard drive
J. A zip drive, 100 USB easy powered (blue)
K. A SanDisk flash drive (4 gigabytes)
L. A Metro PCS cell phone with Micro SD card(black).

ATTACHMENT B

Particular Things to be Seized

All information obtained from the premises will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing information that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 875, 2422(a), 2422(b), 2251(a) and 2252(a)(4)(B) including:

1. Electronic communication, including e-mail, instant messaging and texts;

2. Records evidencing the use of the Internet Protocol address (IP Address);

3. Surveillance footage;

4. Visual images or depictions of Jane Doe or other potential victims;

5. Diaries or diary entries;

6. Calendars or calendar entries;

7. Contracts or confidentiality agreements;

8. Documents containing references to the Newport Mall;

9. Documents containing threats or attempts to extort money or other items of value;

10. Communications and documents related to cellular phones including call logs, text messages, contact lists or calendar entries;

11. Financial documents, including checks, money orders, wires or bank statements and any documents or records related to checks, money orders, wires or bank statements.

12. Images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252(a)(5)(B), in any form wherever they may be

stored or found;

13. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

14. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

15. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

16. Records, information or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, as defined in 18 U.S.C. § 2256, including, but not limited to:

a. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

b. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

17. Billing and payment records, including records from credit card companies, PayPal and other electronic payment services, reflecting access to websites pertaining to child pornography.

18. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

19. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.

20. Records or other items which evidence ownership or use of

computer equipment found in the SUBJECT PREMISES, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

21. Address books, mailing lists, supplier lists, mailing address labels and any and all documents and records pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct.

22. Address books, names, lists of names and addresses of individuals believed to be minors.

23. Diaries, notebooks, notes and other records reflecting personal contact and other activities with individuals believed to be minors.

24. Materials and photographs depicting sexual conduct between adults and minors or used in sexual conduct between adults and minors.

25. Any and all records, documents, invoices and materials that concern any Internet accounts used to possess, receive or distribute child pornography.

26. Evidence of who used, owned, or controlled the PREMISES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence. User attribution information (i.e. files and other data such as chats or e-mails) relevant to the trading of child pornography. Such information tends to show the identity of the person using the computer near the time of the criminal activity;

27. Evidence of software that would allow others to control the PREMISES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

28. Evidence of the lack of such malicious software;

29. Evidence of the attachment to the PREMISES of other storage devices or similar containers for electronic evidence;

30. Evidence of counter-forensic programs (and associated data)

that are designed to eliminate data from the PREMISES;

31. Evidence of the times the PREMISES were used;

32. Passwords, encryption keys, and other access devices that may be necessary to access the PREMISES;

33. Documentation and manuals that may be necessary to access the PREMISES or to conduct a forensic examination of the PREMISES;

34. Evidence of Peer to Peer software;

35. Contextual information necessary to understand the evidence described in this attachment;

If any materials protected by the Privacy Protection Act, 42 U.S.C. § 2000aa are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

36. Records and things evidencing the use of an Internet Protocol address, including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. records of Internet Protocol addresses used;

c. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

37. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein; and

38. Photographs, videos and other images of young women and girls.

Definitions

a. “Child Erotica,” as used herein, means materials and items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene and that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital, oral genital, or oral anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device[.]"

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); and peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information

which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. "Domain name" is a name that identifies an IP address.

j. "Peer to Peer" (also known as "P2P") is a file sharing program that allows people to exchange documents and files between computers. Many of the software programs are available for free on the Internet. When installed, the P2P program allows the installer to designate certain files to share, generally placed in a "shared folder." The files located in the "shared folder" are accessible to anyone who uses the same program by simply searching for specific files and downloading the files. As further detailed below, with regard to the proliferation of child pornography, P2P software, such as "Limewire," "Bearshare," and "Frostwire" are often used to exchange images of child pornography.

k. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures,

photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).